EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"Encryption system resists differential power analysis attacks"	USPAT	OR	ON	2007/08/09 17:00
L2	1	"Encryption system resists differential power analysis attacks"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:11
L3	1	"6937727".pn.	USPAT	OR	ON	2007/08/09 17:10
L4	2	"6937727".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:10
L5	2	"20040047466"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:11
L6	2	"7194090".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:12
L7	2	"20020191784"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:12
L8	2	"20010053220"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:14

EAST Search History

L9	3	"20020027987"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 17:20
S1	0	(10/749412).CCLS.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	OFF	2007/07/22 06:05
S2	0	(10/749412).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/07/22 06:05
S3	0	(10/749412).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/07/22 06:05
S4	1	10/749412	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:22
S5	1335	380/28.ccls.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:23
S6	0	ochi-ryp-$.in.	US-PGPUB; USPAT; USOCR; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:23
S7	0	ochi-ryo-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:24

EAST Search History

S8	11522	ochi-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:24
S9	28	ochi-$.in. AND ryo	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:27
S10	1	kusakabe-susumu-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:27
S11	3420	kusakabe-$.in.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 06:27
S12	300	kusakabe-$.in. AND susumu	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:10
S13	161	encryption SAME (power near analysis)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 07:18
S14	2	"6970561".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 07:22

EAST Search History

S15	2	"6658569".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 07:25
S16	2	"7050581".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 07:25
S21	105	encryption WITH (power near2 analysis)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:25
S22	8	S21 and 713/189.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:18
S23	170	encryption SAME (power near2 analysis)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:26
S25	2061	(380/28-29 OR 380/37).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:29
S26	3876	(380/28-29 OR 380/37 OR 713/193).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:30

EAST Search History

S27	12400	(380/28-30 OR 380/37 380/45-46 380/281 OR 380/277 OR 380/259 OR 713/193 OR 713/189-191 713/300 OR 713/330 OR 726/26). ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:45
S28	376	original near encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/26 10:46
S30	11	divid$4 with encryption NEAR3 sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 06:26
S40	1	10/749412 AND "dummy encryption process"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 12:33
S41	61	divid$4 with encryption with group	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 09:49
S43	27	mix$4 with encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 16:23
S44	1	S41 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 09:45

EAST Search History

S45	35	encryption near process$4 near sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 10:31
S46	2	(encryption near process$4 near sequence) SAME power	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 09:50
S47	0	"09749142"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 10:31
S48	0	"09/749142"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 10:31
S49	48	S near box with (round adj function)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 10:58
S50	1	10/749412 AND (plurality NEAR2 group)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 12:36
S51	1	10/749412 AND (plurality NEAR2 "encryption")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 13:04

EAST Search History

S52	2	"6327661".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 13:28
S53	151	mix$4 NEAR2 encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 13:33
S54	3	mix$4 NEAR2 encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 13:29
S55	12400	(380/28-30 OR 380/37 380/45-46 380/281 OR 380/277 OR 380/259 OR 713/193 OR 713/189-191 713/300 OR 713/330 OR 726/26).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 13:33
S56	41	S53 AND S55	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:00
S57	36	mix$4 ADJ encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:03
S58	21	mix$4 ADJ encryption and sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:04

EAST Search History

S59	1	mix$4 ADJ encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:05
S60	388	(mix$4 combin$4 merg$4)ADJ encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:08
S61	11	(mix$4 combin$4 merg$4)ADJ encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:08
S63	276	S60 AND @ay<="2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:09
S64	387	S60 AND @ay<="20030108"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:09
S65	226	S60 AND @ad<="20030108"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:10
S66	0	S60 AND @ad<="20030108" with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:10

EAST Search History

S67	0	S60 AND @ad<="20030108" SAME sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:10
S68	145	S60 AND @ad<="20030108" AND sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:10
S69	229	encryption WITH ("power analysis" "PA" "SPA" "simple power analysis" "DPA" "differential power analysis")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:55
S70	229	encryption WITH ("power analysis" "PA" "SPA" "simple power analysis" "DPA" "differential power analysis")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 15:55
S71	0	("2007/0140478").URPN.	USPAT	OR	ON	2007/07/30 15:56
S72	0	("2007/0139194").URPN.	USPAT	OR	ON	2007/07/30 15:56
S73	0	("2006/0056622").URPN.	USPAT	OR	ON	2007/07/30 16:03
S74	0	("2004/0096059").URPN.	USPAT	OR	ON	2007/07/30 16:23
S75	381	(mix$4 stir$4 combin$4) ADJ encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 16:24
S76	12	(mix$4 stir$4 combin$4) ADJ encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/30 16:24

EAST Search History

S77	2	"7146499".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:13
S78	1	"7146499".pn. AND ("fake" OR "dummy") WITH data	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:17
S79	939	cipher NEAR algorithm	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:29
S81	989	(380/27 280/28 380/29).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:21
S83	365	(cipher NEAR algorithm) with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:25
S84	9	(cipher NEAR algorithm) with encryption with round	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 08:18
S86	26	(cipher NEAR algorithm) WITH round	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:30

EAST Search History

S88	9	(cipher NEAR algorithm) WITH round with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/02 15:31
S90	2797	block NEAR cipher	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 08:18
S94	47	(block NEAR cipher) WITH round WITH encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 08:43
S98	89	(divid$4 WITH (encrypt$4 WITH "sequence"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:11
S99	89	((divid$4 or seperat$4) WITH (encrypt$4 WITH "sequence"))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:11
S100	15	(encrypt$4 WITH "sequence") WITh ("plurality" OR "many" OR "several") WITH group	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:40
S101	4	S99 and S100	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:13

EAST Search History

S102	1	encryption with sequnce	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:18
S103	3667	encryption with sequence	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:18
S104	989	(380/27 280/28 380/29).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:18
S105	66	S103 and S104	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:19
S106	61	S105 AND @ad<="20030108"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:19
S107	68	(encrypt$4 WITH "sequence") WITh ("plurality" OR "many" OR "several") WITH (group or UNIT)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:43
S108	9	S99 and (encrypt$4 WITH "sequence") WITh ("plurality" OR "many" OR "several") WITH (group or UNIT)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:47

EAST Search History

S109	1	S99 and (encrypt$4 WITH "sequence") WITH (("dummy" OR "fake" OR "false") with data)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 09:50
S110	2	S99 and (encrypt$4 WITH "sequence") WITH (("dummy" OR "fake" OR "false") with encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:00
S111	2	"20010046296"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:04
S112	74	"DES" WITH (dummy OR dummies) WITH data	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:18
S113	553	"DES" WITH (dummy OR dummies)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:18
S114	42	"DES" WITH (dummy OR dummies) with operation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:29
S116	47	"DES" WITH ("dummy" OR dummies OR "fake" OR "fasle") with (operation or calculation)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 10:25

EAST Search History

S131	7677920	"DES" "block cipher"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:29
S132	6827	("DES" "block cipher") WITH round	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:29
S133	196	("DES" "block cipher") WITH round with function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:29
S134	42	("DES" "block cipher") WITH round with function with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:30
S135	2	"5168521".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/05 11:30
S136	2	"5168521".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 15:36
S137	1	10/885148	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 15:36
S138	0	("2005/0055596").URPN.	USPAT	OR	ON	2007/08/08 16:06

EAST Search History

S139	606	dummy NEAR3 processing	USPAT	OR	ON	2007/08/08 16:06
S140	2	dummy NEAR3 processing with encryption	USPAT	OR	ON	2007/08/08 16:08
S141	119	encryption SAME dummy	USPAT	OR	ON	2007/08/08 16:08
S142	0	encryption SAME dummy with round	USPAT	OR	ON	2007/08/08 16:08
S143	0	encryption SAME dummy same round	USPAT	OR	ON	2007/08/08 16:09
S144	1042	block near cipher	USPAT	OR	ON	2007/08/08 16:09
S145	476	(block near cipher) with encryption	USPAT	OR	ON	2007/08/08 16:56
S148	704	round near function	USPAT	OR	ON	2007/08/08 16:10
S149	45	S145 and S148	USPAT	OR	ON	2007/08/08 16:11
S151	2	S145 and S148 and dummy	USPAT	OR	ON	2007/08/08 16:25
S152	0	"200502273631"	USPAT	OR	ON	2007/08/08 16:25
S153	0	"20050273631"	USPAT	OR	ON	2007/08/08 16:26
S154	0	"20050273631"	USPAT	OR	ON	2007/08/08 16:29
S155	1	"7194090".pn.	USPAT	OR	ON	2007/08/08 17:30
S156	1	"6061449 ".pn.	USPAT	OR	ON	2007/08/08 16:39
S157	0	"20060140401"	USPAT	OR	ON	2007/08/08 16:39
S158	0	"System and method for protecting computer software from a white box attack"	USPAT	OR	ON	2007/08/08 16:40
S159	0	"computer software from a white box attack"	USPAT	OR	ON	2007/08/08 16:40
S160	6	"white box attack"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 16:40

EAST Search History

S161	11	(block near cipher) with encryption with round	USPAT	OR	ON	2007/08/08 17:16
S162	2	"20050213756"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 17:10
S163	2	"20030223580"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 17:10
S164	0	(block near cipher) with encryption with dummy	USPAT	OR	ON	2007/08/08 17:16
S165	1	(block near cipher) with encryption same dummy	USPAT	OR	ON	2007/08/08 17:17
S166	1	(block near cipher) same encryption same dummy	USPAT	OR	ON	2007/08/08 17:17
S167	8	(block near cipher) same encryption same dummy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 17:25
S168	9	(block near cipher) same encryption same (dummy or fake or false)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/08 17:45
S169	0	"7194090".pn. AND (dummy WITH "block cipher")	USPAT	OR	ON	2007/08/08 17:30
S170	1	"7194090".pn. AND (dummy)	USPAT	OR	ON	2007/08/08 17:45
S171	0	"7194090".pn. AND (dummy WITH round)	USPAT	OR	ON	2007/08/08 17:45
S172	9	(block near cipher) same dummy	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:23

EAST Search History

S173	0	(S$box near2 excryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:23
S174	0	(S-box near2 excryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:23
S175	53	(S-box near2 encryption)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:23
S176	4	(S-box near2 encryption) with cipher	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:27
S177	2	"6295606".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:28
S178	1	"20070140478"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:36
S179	0	ierative-block	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:36

EAST Search History

S180	5	iterative-block	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:39
S181	4265546	round near S174 function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:39
S182	2291	round near2 function	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:32
S183	57	(round near2 function) near5 cipher	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 06:41
S184	0	("2004/0008841").URPN.	USPAT	OR	ON	2007/08/09 06:42
S185	96	(round near2 function) WITH cipher	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:33
S186	357	round WITH cipher	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:34
S187	110	round WITH cipher with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:40

EAST Search History

S188	992	(380/27 280/28 380/29).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:34
S189	11	S188 and S187	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 08:37
S191	2349	triple NEAR DES	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 09:32
S192	40	S188 AND S191	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 09:32
S193	1	"20040193898" AND random	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 10:00
S194	964494	"AES"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:20
S195	325	"AES" AND Rijndael	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:19

EAST Search History

S196	8	S195 and S188	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:19
S197	964557	"AES" or "Advanced encryption Standard"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:20
S198	5893	("AES" or "Advanced encryption Standard") WITH mix$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:22
S199	21	("AES" or "Advanced encryption Standard") WITH mix$4 with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:21
S200	9422	("AES" or "Advanced encryption Standard") WITH (mix$4 OR compound$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:23
S201	42	("AES" or "Advanced encryption Standard") WITH (mix$4 OR compound$4) same encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 11:32
S202	21	("AES" or "Advanced encryption Standard") WITH (mix$4 OR compound$4) WITH encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 13:11

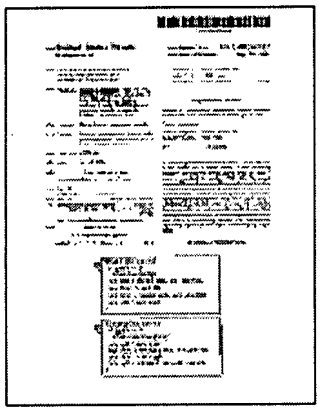
EAST Search History

S203	174	("AES" or "Advanced encryption Standard") WITH (mix$4 OR compound$4) WITH (encryption sequence column)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 13:12
S204	21	("AES" or "Advanced encryption Standard") WITH (mix$4 OR compound$4) WITH (encryption sequence column) with encryption	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 13:12
S205	2	"7236593".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/08/09 13:40
S206	0	("7236593").URPN.	USPAT	OR	ON	2007/08/09 13:44
S208	1	"6937727".pn. and mix$	USPAT	OR	ON	2007/08/09 17:00

Method of scrambling and descrambling data in a communication system

Douglas A. Kuhlman et al

Patent summary



Read this patent

Download PDF

View patent at USPTO

Abstract | Drawing | Description | Claims

Abstract

A scrambling method (510) divides a set of data (200) into a first portion and a second portion. A first scrambling method is performed on the first portion of the set of data to create a scrambled first portion of the data. The second portion of the set of data is modified with the scrambled first portion of the set of data to create a modified second portion of the set of data. A second scrambling method is performed on the modified second portion of the set of data to create a scrambled second portion of the set of data. The scrambled first portion of the set of data is modified with the scrambled second portion of the set of data to create a scrambled set of data (220). A descrambling method (520) reverses the scrambling method (510) to create a descrambed set of data (200).

Patent number: 7099469
Filing date: Oct 17, 2001
Issue date: Aug 29, 2006
Inventors: Douglas A. Kuhlman, Thomas S.

Claims

What is claimed is:

1. A scrambling method for use in a communication system, the method comprising the steps of:

dividing a set of data into a first portion and a second portion;
performing a first scrambling method on the first portion of the set of data to create a scrambled first portion of the data;
modifying the second portion of the set of data with the scrambled first portion of the set of data to create a modified second portion of the set of data;
performing a second scrambling method on the modified second portion of the set of data to create a scrambled second portion of the set of data; and
modifying the scrambled first portion of the set of data with the scrambled second portion of the set of data to create a scrambled set of data, wherein the scrambled set of data is stored in a source device and wherein the first and second scrambling methods recursively execute the above steps until the portion of the set of data to be scrambled reaches a predetermined length.

2. The scrambling method of claim 1 wherein the predetermined length is one byte.

3. The scrambling method of claim 1 further comprising the step of performing a predetermined function on the set of data once the portion of the set of data to be scrambled reaches the predetermined length.

4. The scrambling method of claim 3 wherein the predetermined function is an invertible function.

5. The scrambling method of claim 4 wherein the invertible function is a lookup function.

6. The scrambling method of claim 1 wherein the steps of modifying are invertible.

7. The scrambling method of claim 1 wherein the steps of modifying are selected from a group consisting of: exclusive-or, modular addition, and modular subtraction.

8. The scrambling method of claim 1 further

Google Scholar BETA

Web Images Video News Maps more »

" advanced encryption standard" WITH mixing Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

"WITH" is a very common word and was not included in your search. [details]

Scholar **All articles** - **Recent articles** Results **1** - **10** of about **1,220** for " **advanced encryption stanc**

All Results
R Anderson
I Verbauwhede
L Bassham
E Biham
L Knudsen

Serpent: A Proposal for the **Advanced Encryption Standard** - all 39 versions »
R Anderson, E Biham, L Knudsen - NIST AES Proposal, Jun, 1998 - gel.ulaval.ca
... algorithm, to be called the **Advanced Encryption Standard** or AES ... using 32-fold parallelism during the **encryption** or decryption ... 1. Key **Mixing**: At each round, a 128 ...
Cited by 106 - Related Articles - View as HTML - Web Search

Report on the Development of the **Advanced Encryption Standard** (AES) - all 40 versions »
J Nechvatal, E Barker, L Bassham, W Burr, M ... - Journal of Research of the National Institute of Standards ..., 2001 - cr.yp.to
... graphic community to develop an **Advanced Encryption Standard** (AES ... Both the **mixing**
and the core rounds are ... is a parameterized family of **encryption** ciphers that ...
Cited by 78 - Related Articles - View as HTML - Web Search - BL Direct

... Fair Comparison of the Final Candidates for **Advanced Encryption Standard** Using Field Programmable ... - all 9 versions »
K Gaj, P Chodowiec - Proc. RSA Security Conference-Cryptographer's Track, April, 2001 - Springer
... **Advanced Encryption Standard** (AES) is likely to become a de ... the total area of the **encryption**/decryption unit ... Two of these operations, key **mixing** and linear ...
Cited by 44 - Related Articles - Web Search - BL Direct

Hardware Performance Simulations of Round 2 **Advanced Encryption Standard** Algorithms - all 16 versions »
B Weeks, M Bean, T Rozylowicz, C Ficke - AES3 Conference, April, 2000 - cs-www.ncsl.nist.gov
... performance of the Round 2 **Advanced Encryption Standard** (AES) algorithm ... for the first
round of **encryption** is the ... it is the unkeyed forward **mixing** round result ...
Cited by 47 - Related Articles - View as HTML - Web Search

[BOOK] ... of ANSI C Implementations of Round 1 Candidate Algorithms for the **Advanced Encryption Standard** - all 14 versions »
LE Bassham, National Institute of Standards and ... - 1999 - csrc.nist.gov
... The evaluation criteria for the **Advanced Encryption Standard** (AES) Round1 ... order to
incorporate all key-**mixing** into one ... key setup time and **encryption** speed were ...
Cited by 20 - Related Articles - View as HTML - Web Search - Library Search

... analysis and detection procedures for a hardware implementation of the **advanced encryption standard** - all 8 versions »
G Bertoni, L Breveglieri, I Koren, P Maistri, V ... - IEEE Transactions on Computers, 2003 - doi.ieeecomputersociety.org

Terms used: **advanced encryption standard WITH mixing encryption**

Found **548** of **207,474**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Book reviews: Review of "Data Privacy and Security by David Salomon"; Spring-Verlag, 2003, $51.48, Hardcover.

Nick Papanikolaou

June 2005 **ACM SIGACT News**, Volume 36 Issue 2

Publisher: ACM Press

Full text available: pdf(2.56 MB) Additional Information: full citation, abstract, references, index terms

The field of cryptology and data security hardly needs any introduction; numerous popular accounts of the subject have appeared over the years, and it is already a core topic in undergraduate computer science. The very term "cryptology" is testimony to the long history of the field; the term is derived from the words κονπτός (meaning hidden), and λόγος (meaning speech), which have retained their meaning in the Greek language for many centuries.

2 Embedded systems: applications, solutions and techniques (EMBS): Efficient AES implementations for ARM based platforms

Kubilay Atasu, Luca Breveglieri, Marco Macchetti

March 2004 **Proceedings of the 2004 ACM symposium on Applied computing SAC '04**

Publisher: ACM Press

Full text available: pdf(147.45 KB) Additional Information: full citation, abstract, references, citings

The Advanced Encryption Standard (AES) contest, started by the U.S. National Institute of Standards and Technology (NIST), saw the Rijndael [13] algorithm as its winner [11]. Although the AES is fully defined in terms of functionality, it requires best exploitation of architectural parameters in order to reach the optimum performance on specific architectures. Our work concentrates on ARM cores [1] widely used in the embedded industry. Most promising implementation choices for the common ARM Ins ...

Keywords: AES, ARM microprocessor, cache memories, code optimisation

3 Posters: DRKH: dynamic re-keying with key hopping

Ahmad M. Kholaif, Magda B. Fayek, Hussein S. Eissa, Hoda A. Baraka

October 2005 **Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks PE-WASUN '05**

Publisher: ACM Press